

First Hit Fwd Refs**End of Result Set**☐ **Generate Collection** **Print**

L40: Entry 1 of 1

File: USPT

Apr 24, 2001

DOCUMENT-IDENTIFIER: US 6223285 B1

TITLE: Method and system for transferring information using an encryption mode indicator

Abstract Text (1):

A method and system for transferring information using an encryption mode indicator (EMI). The present invention provides several secure information communication modes in which data (e.g., representing an audio/visual work) can be transmitted from a source device to a sink device (receiving station) in a number of secure modes. In one secure mode, EMI mode A, the information of the transmission is not allowed to be copied as a whole work; this is the highest level of copy protection. In second secure mode, EMI mode B, the information of the transmission is allowed to be copied once and once only by the sink device. In a third transmission mode, no encryption is used and free copying is available. Depending on which secure mode is selected between mode A and mode B, a different encryption process is used by the source device to encrypt the transmission. Further, depending on which secure mode is selected between mode A and mode B, a different decryption process is used by the sink device to decrypt the transmission. The present invention is particularly useful for transmissions between a source device and a bit stream recorder which does not have the capability to extract certain encryption information from a packet header. By using different encryption processes for each transmission mode, an unauthorized device placed between the source and the sink devices that alters the EMI code will be unable to thereafter render or record the audio/visual work because the decryption process selected will differ from the encryption process used.

Brief Summary Text (3):

The present invention relates to the field of information communication systems. More particularly, the present invention relates to the field of secure communication modes for information representing audio/visual works.

Brief Summary Text (5):

In recent years, there has been a technique, by which a plurality of audio/visual (AV) devices can be connected using digital interfaces so that AV information (e.g., representing AV works such as movies, songs, etc.) can be transmitted from an information source (e.g., a video disk player or video cassette recorder) to an information display device (e.g., a television set or monitor) or an information sink device. The development of this technology has led to the adoption of the IEEE 1394 serial communication standard for AV devices. Within the IEEE 1394 serial communication standard, information is transmitted in digital packets having certain header information and having data sections.

Brief Summary Text (6):

The AV digital information that is transmitted (e.g., representing movies) is usually protected by a copyright to prevent unauthorized users from viewing the information and making unauthorized reproductions of the AV works. To prevent unauthorized copying, the AV information is transmitted with encoded copy control information called the Copy Control Information (CCI) bits. The CCI bits can also

be referred to as Copy Generation Management System (CGMS) bits. The encoded CCI code is made up of 2 bits, of which "00," "10," and "11" indicate "unlimited allowance for copies," "allowance for a single generation copy," and "inhibition of copy," respectively. The "01" bit code is left unused. The manner in which the CCI bits are added to an AV information is specified for the different kinds of AV information (e.g., Motion Picture Expert Group MPEG, Digital Video DV and audio data). These CCI bits are added within the data portion of data packets that constitute the AV information to control the use of the AV information by downstream devices.

Brief Summary Text (14):

A method and system are described for transferring information using an encryption mode indicator (EMI). The present invention is useful in applications where copy protected information is to be transferred between devices, e.g., in the transmission of audio/visual works that are subject to copyrights. The present invention can be used within the IEEE 1394 serial communication standard in which transmissions comprise individual packets of information.

Brief Summary Text (15):

The present invention provides several secure information communication modes in which data (e.g., representing an audio/visual work) can be transmitted from a source device to a sink device (receiving station) in a number of secure modes. In one secure mode, EMI mode A, the information of the transmission is not allowed to be copied as a whole work; this is the highest level of copy protection. In second secure mode, EMI mode B, the information of the transmission is allowed to be copied once and once only by the sink device. In a third transmission mode, no encryption is used and free copying is available. Depending on which secure mode is selected between mode A and mode B, a different encryption process is used by the source device to encrypt the transmission. Further, depending on which secure mode is selected between mode A and mode B, a different decryption process is used by the sink device to decrypt the transmission. The EMI code therefore indicates both: (1) the copy protection mode of the transmission; and also (2) the encryption process used.

Brief Summary Text (16):

The present invention is particularly useful for transmissions between a source device and a bit stream recorder which does not have the capability to extract copy control information from a packet header. By using different encryption processes for each transmission mode, an unauthorized device placed between the source and the sink devices that alters the EMI code will be unable to thereafter render or record the audio/visual work because the decryption process selected will differ from the encryption process used.

Drawing Description Text (11):

FIG. 8 illustrates different types of audio/visual devices supported by the present invention and the various communication modes supported by input signals to these devices and output signals from these devices.

Detailed Description Text (7):

System 100 also includes a digital broadcast receiver unit 120. This unit 120 can also be called a set top box (STB). Herein, receiver unit 120 is called the source device 120. The source device 120 contains EMI circuitry 150 in accordance with the present invention to support a number of EMI communication modes which are described further below. Circuit 150 utilizes a different encryption mechanism for each EMI encryption mode. The source unit 120 is an intelligent device and contains specialized circuitry for processing copy protection standards. For instance, source unit 120 receives a digital program over channel 115 and this digital program can be encoded using copy control information (CCI information).

Detailed Description Text (14):

FIG. 4 illustrates the fields that constitute a typical information packet 200 in accordance with the present invention that are sent from the source unit 120 to the sink unit 130 (FIG. 3). Information packet 200 of FIG. 4 contains an IEEE 1394 header section 230 because, in one embodiment, the data packets conform to the IEEE communication standard. This header section 230 contains a data_length field, a tag field, a channel field, a tcode field and an sy field. Aside from the tag and tcode fields, header 230 conforms to the well known IEEE standard and the other fields are defined therein. The tag field indicates that the data field starts with a CIP header 240. The tcode field can be one of two predetermined values. It is appreciated that a data stream means a stream of information on one 1394 isochronous channel.

Detailed Description Text (16):

EMI modes within field 210 indicate the copy control status of the data stream on the 1394 isochronous stream. It is important to understand that the data stream in accordance with the present invention can consist of several video and/or audio programs and each of them can have a different copy control information associated with the program. For instance, the MPEG transport stream output from a source unit can contain several programs, each of which can have a different level of copy protection. The source device assigns the EMI value for the most restrictive program in the stream. A bit stream recorder may or may not record the entire stream based on the EMI value. Another type of recording device which is capable of processing each program in the stream individually and is also capable of interpreting copy control information associated with each program is called a format cognizant recording device. A format cognizant recording device refers control information associated with each program to decide its action.

Detailed Description Text (18):

FIG. 5A illustrates a system 400 of the present invention having a source device 120 and a sink device 130. FIG. 5A illustrates the EMI circuitry 150 of a typical source unit 120 in more detail. Source unit 120 can be a set-top-box (STB) unit also called a broadcast receiver which contains many well known circuits (not shown for clarity) in addition to the EMI circuit 150. A receiver circuit 410 receives AV information in the form of data packets and performs any decryption required under CCI standards. The result is forwarded over communication interface 430 and also to a de-multiplexer (de-mux) 414 using interface 413. Circuit 412 is an EMI mode select circuit and depending on the recovered CCI copy protection information will select either EMI mode A or EMI mode B, if copy protection is required. If no copy protection is required, then interface 413 is passed directly to interface 125 and EMI mode O (code "00") is inserted into EMI field 210 of the data packet.

Detailed Description Text (25):

Source unit 120' of FIG. 5B can be a set-top-box (STB) unit also called a broadcast receiver which contains many well known circuits (not shown for clarity) in addition to EMI circuit 150'. A receiver circuit 510 receives AV information in the form of a data packet and performs any decryption required under CCI standards. The result is forwarded over communication interface 512 (coupled to an EMI mode selected circuit 514) and also to an interface 513. Circuit 514 is an EMI mode select circuit and depending on the recovered CCI copy protection information will select either EMI mode A or EMI mode B, if copy protection is required. If no copy protection is required, then interface 513 is passed directly to interface 125 and EMI mode O (code "00") is inserted into EMI field 210 of the data packet.

CLAIMS:

5. A system as described in claim 1 wherein said information packet represents a portion of a digital audio/visual program.

11. A system as described in claim 8 wherein said information packet represents a portion of a digital audio/visual program.

16. A system as described in claim 12 wherein said information packet represents a portion of a digital audio/visual program.

[First Hit](#) [Fwd Refs](#)**End of Result Set**☐ **Generate Collection** **Print**

L40: Entry 1 of 1

File: USPT

Apr 24, 2001

DOCUMENT-IDENTIFIER: US 6223285 B1

TITLE: Method and system for transferring information using an encryption mode indicator

Abstract Text (1):

A method and system for transferring information using an encryption mode indicator (EMI). The present invention provides several secure information communication modes in which data (e.g., representing an audio/visual work) can be transmitted from a source device to a sink device (receiving station) in a number of secure modes. In one secure mode, EMI mode A, the information of the transmission is not allowed to be copied as a whole work; this is the highest level of copy protection. In second secure mode, EMI mode B, the information of the transmission is allowed to be copied once and once only by the sink device. In a third transmission mode, no encryption is used and free copying is available. Depending on which secure mode is selected between mode A and mode B, a different encryption process is used by the source device to encrypt the transmission. Further, depending on which secure mode is selected between mode A and mode B, a different decryption process is used by the sink device to decrypt the transmission. The present invention is particularly useful for transmissions between a source device and a bit stream recorder which does not have the capability to extract certain encryption information from a packet header. By using different encryption processes for each transmission mode, an unauthorized device placed between the source and the sink devices that alters the EMI code will be unable to thereafter render or record the audio/visual work because the decryption process selected will differ from the encryption process used.

Brief Summary Text (3):

The present invention relates to the field of information communication systems. More particularly, the present invention relates to the field of secure communication modes for information representing audio/visual works.

Brief Summary Text (5):

In recent years, there has been a technique, by which a plurality of audio/visual (AV) devices can be connected using digital interfaces so that AV information (e.g., representing AV works such as movies, songs, etc.) can be transmitted from an information source (e.g., a video disk player or video cassette recorder) to an information display device (e.g., a television set or monitor) or an information sink device. The development of this technology has led to the adoption of the IEEE 1394 serial communication standard for AV devices. Within the IEEE 1394 serial communication standard, information is transmitted in digital packets having certain header information and having data sections.

Brief Summary Text (6):

The AV digital information that is transmitted (e.g., representing movies) is usually protected by a copyright to prevent unauthorized users from viewing the information and making unauthorized reproductions of the AV works. To prevent unauthorized copying, the AV information is transmitted with encoded copy control information called the Copy Control Information (CCI) bits. The CCI bits can also

be referred to as Copy Generation Management System (CGMS) bits. The encoded CCI code is made up of 2 bits, of which "00," "10," and "11" indicate "unlimited allowance for copies," "allowance for a single generation copy," and "inhibition of copy," respectively. The "01" bit code is left unused. The manner in which the CCI bits are added to an AV information is specified for the different kinds of AV information (e.g., Motion Picture Expert Group MPEG, Digital Video DV and audio data). These CCI bits are added within the data portion of data packets that constitute the AV information to control the use of the AV information by downstream devices.

Brief Summary Text (14):

A method and system are described for transferring information using an encryption mode indicator (EMI). The present invention is useful in applications where copy protected information is to be transferred between devices, e.g., in the transmission of audio/visual works that are subject to copyrights. The present invention can be used within the IEEE 1394 serial communication standard in which transmissions comprise individual packets of information.

Brief Summary Text (15):

The present invention provides several secure information communication modes in which data (e.g., representing an audio/visual work) can be transmitted from a source device to a sink device (receiving station) in a number of secure modes. In one secure mode, EMI mode A, the information of the transmission is not allowed to be copied as a whole work; this is the highest level of copy protection. In second secure mode, EMI mode B, the information of the transmission is allowed to be copied once and once only by the sink device. In a third transmission mode, no encryption is used and free copying is available. Depending on which secure mode is selected between mode A and mode B, a different encryption process is used by the source device to encrypt the transmission. Further, depending on which secure mode is selected between mode A and mode B, a different decryption process is used by the sink device to decrypt the transmission. The EMI code therefore indicates both: (1) the copy protection mode of the transmission; and also (2) the encryption process used.

Brief Summary Text (16):

The present invention is particularly useful for transmissions between a source device and a bit stream recorder which does not have the capability to extract copy control information from a packet header. By using different encryption processes for each transmission mode, an unauthorized device placed between the source and the sink devices that alters the EMI code will be unable to thereafter render or record the audio/visual work because the decryption process selected will differ from the encryption process used.

Drawing Description Text (11):

FIG. 8 illustrates different types of audio/visual devices supported by the present invention and the various communication modes supported by input signals to these devices and output signals from these devices.

Detailed Description Text (7):

System 100 also includes a digital broadcast receiver unit 120. This unit 120 can also be called a set top box (STB). Herein, receiver unit 120 is called the source device 120. The source device 120 contains EMI circuitry 150 in accordance with the present invention to support a number of EMI communication modes which are described further below. Circuit 150 utilizes a different encryption mechanism for each EMI encryption mode. The source unit 120 is an intelligent device and contains specialized circuitry for processing copy protection standards. For instance, source unit 120 receives a digital program over channel 115 and this digital program can be encoded using copy control information (CCI information).

Detailed Description Text (14):

FIG. 4 illustrates the fields that constitute a typical information packet 200 in accordance with the present invention that are sent from the source unit 120 to the sink unit 130 (FIG. 3). Information packet 200 of FIG. 4 contains an IEEE 1394 header section 230 because, in one embodiment, the data packets conform to the IEEE communication standard. This header section 230 contains a data_length field, a tag field, a channel field, a tcode field and an sy field. Aside from the tag and tcode fields, header 230 conforms to the well known IEEE standard and the other fields are defined therein. The tag field indicates that the data field starts with a CIP header 240. The tcode field can be one of two predetermined values. It is appreciated that a data stream means a stream of information on one 1394 isochronous channel.

Detailed Description Text (16):

EMI modes within field 210 indicate the copy control status of the data stream on the 1394 isochronous stream. It is important to understand that the data stream in accordance with the present invention can consist of several video and/or audio programs and each of them can have a different copy control information associated with the program. For instance, the MPEG transport stream output from a source unit can contain several programs, each of which can have a different level of copy protection. The source device assigns the EMI value for the most restrictive program in the stream. A bit stream recorder may or may not record the entire stream based on the EMI value. Another type of recording device which is capable of processing each program in the stream individually and is also capable of interpreting copy control information associated with each program is called a format cognizant recording device. A format cognizant recording device refers control information associated with each program to decide its action.

Detailed Description Text (18):

FIG. 5A illustrates a system 400 of the present invention having a source device 120 and a sink device 130. FIG. 5A illustrates the EMI circuitry 150 of a typical source unit 120 in more detail. Source unit 120 can be a set-top-box (STB) unit also called a broadcast receiver which contains many well known circuits (not shown for clarity) in addition to the EMI circuit 150. A receiver circuit 410 receives AV information in the form of data packets and performs any decryption required under CCI standards. The result is forwarded over communication interface 430 and also to a de-multiplexer (de-mux) 414 using interface 413. Circuit 412 is an EMI mode select circuit and depending on the recovered CCI copy protection information will select either EMI mode A or EMI mode B, if copy protection is required. If no copy protection is required, then interface 413 is passed directly to interface 125 and EMI mode O (code "00") is inserted into EMI field 210 of the data packet.

Detailed Description Text (25):

Source unit 120' of FIG. 5B can be a set-top-box (STB) unit also called a broadcast receiver which contains many well known circuits (not shown for clarity) in addition to EMI circuit 150'. A receiver circuit 510 receives AV information in the form of a data packet and performs any decryption required under CCI standards. The result is forwarded over communication interface 512 (coupled to an EMI mode selected circuit 514) and also to an interface 513. Circuit 514 is an EMI mode select circuit and depending on the recovered CCI copy protection information will select either EMI mode A or EMI mode B, if copy protection is required. If no copy protection is required, then interface 513 is passed directly to interface 125 and EMI mode O (code "00") is inserted into EMI field 210 of the data packet.

CLAIMS:

5. A system as described in claim 1 wherein said information packet represents a portion of a digital audio/visual program.

11. A system as described in claim 8 wherein said information packet represents a portion of a digital audio/visual program.

16. A system as described in claim 12 wherein said information packet represents a portion of a digital audio/visual program.